CLAIMS

What is claimed is:

1 A method for providing a secure data storage system, wherein the data storage system is accessed by a processor, the method comprising the steps of:

(a) creating a plurality of logical partitions;

(b) creating a backup partition and backing up the logical partitions to the backup partition;

(c) hiding the backup partition from the processor; and

(d) automatically blocking low-level physical drive write commands, thereby preventing a virus from using such a command to destroy data on the logical and backup partitions.

2 The method of claim 1 further including the step of providing the data storage system as a RAID system wherein a RAID controller is coupled between the processor and a disk drive system containing the logical partitions and the backup partition.

3 The method of claim 1 wherein step (d) further includes the step of: providing the RAID controller with a write flag to block and unblock the low-level physical drive write commands, and defaulting the write flag to a block setting at system reboot.

4 The method of claim 3 wherein step (d) further includes the step of:

requiring a utility that utilizes the low-level physical drive write commands to first issue an unblock write command to the RAID controller prior to issuing a low-level physical drive write command in order to set the write flag to unblock; and

upon completion of the low-level physical drive write command, requiring the utility to issue a block write command to the RAID controller to re-block the low-level write command by setting the write flag to block.

5 The method of claim 4 wherein step (d) further includes the steps of: password protecting the block/unblock write command issued by the utility.

6 The method of claim 5 wherein step (d) further includes the step of: enabling backup partition configuration by both a user and program control during normal operation.

7 The method of claim 6 wherein step (d) further includes the step of: passing a password entered by a user at a prompt of the utility to the RAID controller with the block/unblock command.

8 The method of claim 3 wherein step (d) further includes the step of: storing the write flag as part of the RAID configuration attributes within the RAID controller.

9 The method of claim 5 wherein step (d) further includes the step of: storing the write flag and a user password for the block/unblock write command in an NVRAM.

10 The method of claim 1 further including the steps of: using a software utility to enable a user to create the logical partitions and a backup partition, and to use a hide/unhide logical partition command to hide and unhide the backup partition.

11 The method of claim 10 further including the step of: password protecting the hide/unhide logical partition command.

12 The method of claim 11 further including the step of: storing the password for the hide/unhide logical partition command in an NVRAM.

13 The method of claim 10 further including the steps of:

(e) after one or more of the logical partitions has been corrupted, allowing a user to boot the system using the utility software;

(f) sending a user entered password and the unhide logical partition command to the RAID controller, and unhiding the backup partition if the password is verified; and

(g) restoring the corrupted logical partition from the backup partition.

14 A data storage system comprising,

a processor for executing programs;

a disk drive system divided into logical partitions and a backup partition, the backup partition for backing up the logical partitions, and wherein the backup partition is hidden from the processor; and

a controller coupled between the processor and the disk drive system, the controller including a write flag for blocking and unblocking physical drive write commands, wherein the write flag defaults to a block setting at system reboot and is configurable during normal system operation by a program executing on the processor via a user password-protected block/unblock command.

15 The system of claim 14 wherein a utility that utilizes the low-level physical drive write commands first issues an unblock write command to the RAID controller prior to issuing a low-level physical drive write command in order to set the write flag to unblock, and upon completion of the low-level physical drive write command, issues a block write command to the RAID controller to re-block the low-level write command by setting the write flag to block.

16 The system of claim 15 wherein the block/unblock write command issued by the utility is password protected.

17 The system of claim 16 wherein a password entered by a user at a prompt of the utility is passed to the RAID controller with the block/unblock command.

18 The system of claim 17 wherein the write flag is stored as part of the RAID configuration attributes within the RAID controller.

19 The system of claim 18 wherein the write flag and a user password for the block/unblock write command is stored in an NVRAM.

20 The system of claim 14 further including a software utility to enable a user to create the logical partitions and the backup partition, and to use a hide/unhide logical partition command to hide and unhide the backup partition.

21 The system of claim 20 wherein the hide/unhide logical partition command is password protected.

22 The system of claim 21 wherein the password for the hide/unhide logical partition command is stored in an NVRAM.

23 The system of claim 20 wherein after one or more of the logical partitions has been corrupted, the user boots the system using the utility software, the user entered password and the unhide logical partition command is sent to the RAID controller, the backup partition is unhidden if the password is verified, and the corrupted logical partition is restored from the backup partition.

24 A computer-readable medium containing programs instructions for providing a

secure data storage system, wherein the data storage system is accessed by a processor, the instructions for:

(a) creating a plurality of logical partitions;

(b) creating a backup partition and backing up the logical partitions to the backup partition;

(c) hiding the backup partition from the processor; and

(d) automatically blocking low-level physical drive write commands, thereby preventing a virus from using such a command to destroy data on the logical and backup partitions.

25 The computer-readable medium of claim 24 further including the instruction of providing the data storage system as a RAID system wherein a RAID controller is coupled between the processor and a disk drive system containing the logical partitions and the backup partition.

26 The computer-readable medium of claim 24 wherein instruction (d) further includes the instruction of: providing the RAID controller with a write flag to block and unblock the low-level physical drive write commands, and defaulting the write flag to a block setting at system reboot.

27 The computer-readable medium of claim 26 wherein instruction (d) further includes the instruction of:

requiring a utility that utilizes the low-level physical drive write commands

to first issue an unblock write command to the RAID controller prior to issuing a low-level physical drive write command in order to set the write flag to unblock; and

upon completion of the low-level physical drive write command, requiring the utility to issue a block write command to the RAID controller to re-block the low-level write command by setting the write flag to block.

28 The computer-readable medium of claim 27 wherein instruction (d) further includes the instructions of: password protecting the block/unblock write command issued by the utility.

29 The computer-readable medium of claim 28 wherein instruction (d) further includes the instruction of: enabling backup partition configuration by both a user and program control during normal operation.

30 The computer-readable medium of claim 29 wherein instruction (d) further includes the instruction of: passing a password entered by a user at a prompt of the RAID utility to the RAID controller with the block/unblock command.

31 The computer-readable medium of claim 26 wherein instruction (d) further includes the instruction of: storing the write flag as part of the RAID configuration attributes within the RAID controller.

32 The computer-readable medium of claim 28 wherein instruction (d) further includes the instruction of: storing the write flag and a user password for the block/unblock write commands in an NVRAM.

33 The computer-readable medium of claim 24 further including the instructions of: using a software utility to enable a user to create the logical partitions and a backup partition, and to use a hide/unhide logical partition command to hide and unhide the backup partition.

34 The computer-readable medium of claim 33 further including the instruction of: password protecting the hide/unhide logical partition command.

35 The computer-readable medium of claim 34 further including the instruction of: storing the password for the hide/unhide logical partition command in an NVRAM.

36 The computer-readable medium of claim 33 further including the steps of:

(e) after one or more of the logical partitions has been corrupted, allowing a user to boot the system using the utility software;

(f) sending a user entered password and the unhide logical partition command to the RAID controller, and unhiding the backup partition if the password is verified; and

(h) restoring the corrupted logical partition from the backup partition.